Federal Bureau of Investigation

Privacy Impact Assessment
for the
Enterprise Telecommunications Infrastructure System

Issued by:
Erin M. Prest, Privacy and Civil Liberties Officer

Approved by: Peter A. Winn, Acting Chief Privacy and Civil Liberties Officer, U.S. Department of Justice

Date approved: September 30, 2018

(May 2015 DOJ PIA Form)

(U) EXECUTIVE SUMMARY

(U) The Enterprise Telecommunications Infrastructure System (ETIS)[1] provides call delivery to all personnel located at the Criminal Justice Information System (CJIS) Division[2] and common areas as well as business entities within CJIS, including the National Instant Criminal Background Check System (NICS), the Public Access Line (PAL)[3], the Biometric Services Section (BSS) Customer Service Group (CSG), the Major Case Contact Center (MC3), and the CJIS Help Desk and Switchboard Operations. The ETIS maintains a log of all incoming and outgoing phone calls from CJIS. For the business entities listed above, the ETIS also captures an audio recording of the phone call. The call information is stored in a call log database with the audio recording of the call. The ETIS also maintains a directory of all CJIS extensions and the name of the individual to whom the extension is assigned. This Privacy Impact Assessment is being completed to discuss the privacy impact for maintaining caller identification information and the audio file recordings of telephone calls.

(U) Section 1: Description of the Information System

(U) (a) The purpose that the records and/or system are designed to serve;

(U) The ETIS facilitates communications inside and outside of the CJIS Division. It is the phone system for CJIS and links together all communications within the CJIS Division. For administrative purposes, the ETIS maintains logs of calls placed and received. To meet the business needs of the entities listed above, the ETIS maintains call logs and audio recordings of telephone calls.

(U) (b) The way the system operates to achieve the purpose(s);

(U) The ETIS provides call delivery to all CJIS personnel and common areas and maintains a record of all telephonic communication into and out of CJIS. The ETIS logs all incoming and outgoing phone calls from CJIS. The ETIS also provides call delivery to business entities at CJIS. To meet the operational needs of the CJIS Division, the ETIS records all incoming phone calls made to the following business entities within CJIS:

(U) The National Instant Criminal Background Check System (NICS)[4]: NICS is a national name check system that queries available records in federal and state databases to determine if prospective purchasers of firearms are disqualified from receiving firearms. The NICS Customer Service Representatives (CSRs) receive requests via phone calls from Federal Firearms Licensees (FFL). FFLs calling NICS for firearm transactions provide their FFL license number and assigned

[1] During development, this project was referred to as the Telecommunications Infrastructure Upgrade (TIU). Its operational name is Enterprise Telecommunications Infrastructure Systems (ETIS).
[2] Personnel at the CJIS Division include FBI employees, contractors, and detailees as well as other federal agency liaisons stationed at the CJIS Division.
[3] The PAL unit also answers calls made to the FBI's Weapons of Mass Destruction Directorate (WMDD).
[4] NICS has separate privacy documentation and is covered by its own system of records notice, FBI-018.

codeword. Once the NICS CSR validates the FFL's information, the FFL provides personally identifiable information (PII) supplied by the firearm purchaser. This information includes the purchaser's name and date of birth and may also include the purchaser's social security number. The CSR initiates the background check with the firearm purchaser's information. If the NICS provides no negative hits, the CSR authorizes the FFL to proceed with the gun sale. Not all NICS checks are resolved during this telephone call because sometimes additional research is required. The ETIS records all incoming calls to the NICS customer service centers. These calls are recorded for quality assurance purposes and are retained for 24 hours. During this 24 hour period, authorized NICS employees can access the call recordings by logging into specialized software within the ETIS and retrieving the call by CSR name or agent identification number, automatic number identifier (ANI),[5] or date and time of the call.

(U) The Public Access Line (PAL): PAL is a national telephone call center that serves as the FBI's central intake for information and "tips" from members of the public regarding potential violations of criminal law and threats to national security. The PAL Unit provides 24/7 telephone line support, using the Public Access Line Manager (PALM) [6] database to collect "tip" information and forward appropriate lead information to investigators. The PAL unit also processes calls for the Major Case Contact Center (MC3), which provides centralized case support of "tip" line information and coordinates with law enforcement agencies to support security and investigations during major cases and catastrophic events. The MC3 is utilized when a high volume of calls is expected and the Field Offices do not have sufficient staff to handle anticipated call volume. For example, the MC3 may be activated when the FBI is looking for a fugitive or when a terrorist attack has occurred. Additionally, the PAL unit processes calls for the Weapons of Mass Destruction Directorate (WMDD), which integrates and links all FBI counterterrorism, intelligence, counterintelligence, and scientific and technological components to accomplish the FBI's mission to prevent and to respond to any terrorist threat or incident in the United States involving Weapons of Mass Destruction (WMD) consisting of chemical, biological, or radiological material. The PAL unit answers telephone calls to the FBI WMDD toll-free telephone number.

(U) The PAL Unit CSRs answer all telephone calls to the FBI tips toll-free telephone number, the MC3, and the WMDD. CSRs collect information from callers and enter the information into the PALM. Callers may provide their name or other identifying information, or the call may be anonymous. Callers to the PAL may provide PII on other individuals about whom the caller is giving a tip to the FBI. The ETIS records all incoming calls to the PAL for quality assurance, record keeping, and investigatory purposes. Occasionally, PAL CSRs make outbound calls for official purposes to obtain additional information from individuals who submitted tips to the PAL Unit.[7] When the CSR makes a return call for official purposes, the CSR records the phone call by pressing a button on the

---

[5] The ANI is the phone number from which the call initiates. If the call is transferred from a field office that does not pass the ANI, the ETIS captures the main number of the field office. If the call is not initiated or transferred from a field office and the caller is not blocking his caller ID, the ETIS captures the phone number from which the caller placed the phone call. The ETIS only captures the ANI; the ETIS system does not capture the caller's name.

[6] PALM has separate privacy documentation.

[7] The practice of making outbound calls from the PAL unit for official purposes is rare and discouraged.

phone. This recording is necessary in order to adequately document any additional information the caller may provide. All outbound/return calls are initiated for follow-up purposes only as a result of a previously received tip. All calls recorded for the PAL are retained for five years. Calls remain within the ETIS for 13 months. After 13 months, calls can be restored to the ETIS from backup storage. Calls recorded for PAL may be sent to investigators following up on a tip from PAL. To retrieve a call recording from the ETIS, authorized PAL employees log into specialized software in the ETIS and retrieve the call by the universal call identification (UCID) number associated with the tip in PALM. Call recordings can also be retrieved by CSR name or agent identification number, ANI, or date and time of the call. Authorized PAL employees can also retrieve calls from the ETIS directly from the PALM database by clicking a player button. The player button pulls the call recording from the ETIS for playback.

(U) The Biometric Services Section (BSS) Customer Service Group (CSG): BSS CSG provides biometric identification services, including the processing of fingerprint submissions and criminal history records within the Next Generation Identification (NGI) system.[8] The BSS CSG receives telephone calls from the public and biometric information system users regarding updates on requests for criminal history records and fingerprint queries. Callers to the BSS CSG may provide PII on individuals to assist the CSR in locating records in the NGI system. The data provided by the callers to the BSS CSG may contain PII such as name, universal control number (UCN),[9] social security number, and date of birth. This information is not maintained within ETIS other than in the audio recording of the call. All recorded calls to the BSS CSG are saved for 30 days for record keeping and quality assurance purposes. Authorized BSS CSG employees retrieve call recordings from the ETIS by logging into specialized software within the ETIS. Call recordings can be retrieved by CSR name or agent identification number, ANI, or date and time of the call.

(U) The CJIS Help Desk and Switchboard Operations: The CJIS Help Desk receives telephone calls and provides assistance to individuals utilizing CJIS services. The Switchboard answers calls to the main CJIS phone number, as well as calls to the main FBI headquarters phone number on nights, weekends, and holidays, and directs callers to the appropriate individual or program. All inbound calls to the CJIS Help Desk and the Switchboard are recorded and saved for quality assurance purposes for 30 days. Authorized Help Desk and Switchboard employees retrieve call recordings from the ETIS by logging into specialized software within the ETIS. Call recordings can be retrieved by CSR name or agent identification number, ANI, or date and time of the call.

(U) Only the CJIS business entities listed above have the ability to record telephone calls. CJIS personnel at their desks or in common areas do not have call recording capabilities. All of the business entities that record calls notify callers in advance that their call may be recorded or monitored.

---

[8] NGI has separate privacy documentation.
[9] The UCN, also known as an FBI number, is a unique identification number assigned to each fingerprint submission to NGI.

(U) (c) The type of information collected, maintained, used, or disseminated by the system;

(U) The ETIS maintains a log of all incoming and outgoing phone calls from CJIS. When a phone call comes into CJIS, the ETIS captures the date and time of the call, the ANI of the originating caller, the extension of the CJIS workstation answering the call as well as the name of the individual to whom the extension is assigned, and the length of the call. For outgoing calls, the ETIS captures the extension of the CJIS workstation making the call as well as the name of the individual to whom the extension is assigned, the number called, the date and time of the call, and the duration of the call. For the business entities listed above, the ETIS also captures an audio recording of the phone call. The call information is stored in a call log database with the audio recording of the call. The ETIS also maintains a directory of all CJIS extensions and the name of the individual to whom the extension is assigned. Call log information is maintained within the ETIS. The call log information for the last 100 calls to and from a CJIS workstation is also saved locally on the desk phone. If employees are logged into a call center, the call log information is maintained within the ETIS. For contact information and administrative purposes, the ETIS also maintains a phone directory containing CJIS personnel's names and the phone extensions assigned to each individual.

(U) Information contained within the ETIS call recordings for the various business entities differs based on the business entity for which the call is recorded. As discussed above, **NICS** receives calls from FFLs. FFLs calling NICS for firearm transactions provide their FFL license number and assigned codeword. Once the NICS CSR validates the FFL's information, the FFL provides PII supplied by the firearm purchaser. This information includes the purchaser's name and date of birth and may also include the purchaser's social security number.

(U) CSRs from the **PAL** Unit collect information from callers and enter the information into the PALM. Callers may provide their name or other identifying information, or the call may be anonymous. Callers to the PAL may provide PII on other individuals about whom the caller is giving a tip to the FBI.

(U) Callers to the **BSS CSG** may provide PII on individuals to assist the CSR in locating records in the NGI system. The data provided by the callers to the BSS CSG may contain PII such as name, UCN, social security number, and date of birth.

(U) (d) Who has access to information in the system

(U) Access to the information within the ETIS is restricted based upon an individual's status as a user. General users include all personnel at the CJIS Division who are not logged into a call center. General users have access to the physical phones at their workstation. Through the physical phone, general users can access the internal phone directory and the call log for their assigned extension. A user's call log retains a record of the last 100 calls to or from the extension. The call log provides the name of the individual calling the extension (if the individual is an internal user), the number from which the call originated (if the number is not blocked), the time and date of the call, and the length of the call. From the call log, general users can add individuals as contacts and call individuals. General

users have the ability to clear the call log from their physical phone; however, the call log remains within the ETIS.

(U) Privileged users of the ETIS include system administrators, application administrators, and system security administrators. Each privileged user type has different access to the information within the ETIS:

(U) System Administrators administer the ETIS and have the ability to troubleshoot the system, restart servers and services, and implement both environmental and functional system changes. System Administrators have access to the call logs and phone directories within the ETIS.

(U) Application Administrators support the multiple application-level services including over a dozen key applications to maintain the ETIS project. A few key select application administrators control, access, and make decisions related to implementation and management of the call recording services. Application administrators monitor, troubleshoot, and assist business entities with accessing call recordings and using the ETIS' specialized software.

(U) System Security Administrators (SSAs) have primary responsibility for administering system security functions, managing user IDs and user accounts, and performing monitoring of security audit records. SSAs work closely with system administrators to maintain the system and to monitor system changes and user activity.

(U) Call recordings may be accessed by authorized privileged users and authorized users from the business entities based on different tiered levels of security access controls which are controlled by the business entity to which the call was directed. A business entity cannot see another's business entity's call recordings at the end-user level. For example, calls recorded for PAL cannot be viewed by the BSS CSG.

(U) (e) How information in the system is retrieved by the user;

(U) To access a call recording, a designated authorized user within a business entity logs into specialized software within the ETIS. The specialized software allows authorized users to access the calls for their business entity. Users can search for call recordings by CSR name or agent identification number, date and time of call, or ANI (if available). For calls into the PAL, call recordings are also searchable by the UCID. The specialized software allows authorized users to listen to the call recording. ETIS software also allows business entities to review a small subset of recorded calls for quality purposes. Authorized PAL users can also retrieve call recordings directly from the PALM database by clicking the player button. The player button pulls the call recording from the ETIS for playback. If necessary for the business entity, the authorized user can download the call for further use consistent with the business entity's needs. Once downloaded, the call recording leaves the ETIS and is controlled by the business entity's established processes for handling call recording information.

(U) Call log information in the ETIS can be retrieved by any data element in the call log. General users can search the ETIS phone directory on their desk phone by first and last name.

(U) (f) How information is transmitted to and from the system;

(U) The ETIS uses Voice over Internet Protocol (VOIP) technology to route phone calls received via dedicated integrated services digital network (ISDN) transmission system 1 (T1) lines. Public callers place their calls from any type of telephone. The calls are routed to the CJIS infrastructure via the Public Switched Telephone Network (PSTN) and encrypted upon receipt of the call within the CJIS ETIS infrastructure. Incoming calls placed to the main CJIS phone number are greeted with an Interactive Voice Response (IVR) system that receives the incoming phone calls from the public and redirects the request to the appropriate CSR following a series of inquiry prompts.

(U) (g) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects);

(U) The ETIS system is contained within the CJIS Shared Enterprise Network (SEN).[10] Call recordings and information are only resident on the CJIS SEN while in transit. Call log information is stored within the ETIS. Call recordings are stored encrypted in digital format within the Enterprise Storage Area Network (ESAN). The phone directory accessible to CJIS employees pulls information from the ETIS communications manager database. The phone directory provides the name and desk phone number of personnel at the CJIS Division.

(U) When PAL CSRs answer phone calls, the PALM Database pulls information from ETIS into the PALM database (e.g. UCID, ANI) to create a PALM call entry. Authorized users in PAL can also pull call recordings from ETIS into the PALM database via the player button.

(U) (h) Whether it is a general support system, major application, or other type of system.

(U) The ETIS is categorized as an information system.

[10] CJIS SEN has its own privacy documentation.

(U) Section 2: Information in the System

2.1 (U) Indicate below what information is collected, maintained, or disseminated. (Check all that apply.)

(U) Identifying numbers					
Social Security		Alien Registration		Financial account	
Taxpayer ID		Driver's license		Financial transaction	
Employee ID		Passport		Patient ID	
File/case ID		Credit card			
Other identifying numbers (specify): (U) The ETIS does not require social security numbers or other identifying numbers; however, individuals calling CJIS business entities may provide the above information to CSRs during a call. Therefore, audio recordings of calls captured by the ETIS may contain social security numbers or other identifying numbers. Call recordings cannot be searched or retrieved by information provided verbally during a call.					

(U) General personal data					
Name	X	Date of birth		Religion	
Maiden name		Place of birth		Financial info	
Alias		Home address		Medical information	
Gender		Telephone number	X	Military service	
Age		Email address		Physical characteristics	
Race/ethnicity		Education		Mother's maiden name	
Other general personal data (specify): (U) The ETIS call logs and phone directory contain only names of personnel at the CJIS Division and telephone numbers. Additional general personal data may be provided by callers to CSRs, and therefore may be contained within audio recordings captured by the ETIS. However, call recordings cannot be searched or retrieved by information provided verbally during a call.					

(U) Work-related data					
Occupation		Telephone number	x	Salary	
Job title		Email address		Work history	
Work address		Business associates			
Other work-related data (specify): (U) The ETIS call logs and phone directory contain names of CJIS employees and telephone numbers. Additional work-related data may be provided by callers to CSRs, and therefore may be contained within audio recordings captured by the ETIS. However, call recordings cannot be searched or retrieved by information provided verbally during a call.					

(U) Distinguishing features/Biometrics					
Fingerprints		Photos		DNA profiles	
Palm prints		Scars, marks, tattoos		Retina/iris scans	
Voice recording/signatures	X	Vascular scan		Dental profile	
Other distinguishing features/biometrics (specify): (U) The call recordings naturally include voice recordings of CSRs and callers; however, the voice recordings are not searchable by voice signature.					

(U) System admin/audit data					
User ID	X	Date/time of access	X	ID files accessed	X
IP address		Queries run		Contents of files	
Other system/audit data (specify): (U) The ETIS call recorder generates audit records for replay of call recordings via most ETIS software that includes a unique ID number for the call recording replayed. This permits the ability to identify which calls were replayed.					

Other information (specify)

2.2 (U) Indicate sources of the information in the system. (Check all that apply.)

(U) Directly from individual about whom the information pertains					
In person		Hard copy: mail/fax	X	Online	
Telephone	X	Email			
Other (specify): (U) The phone directory includes names and phone extensions from personnel at the Division which is provided directly by the individual, via internal mail/fax, to receive a phone account. All call log information and information within call recordings is provided by telephone.					

(U) Government sources					
Within the Component	X	Other DOJ components	x	Other federal entities	x
State, local, tribal	x	Foreign	x		
Other (specify): (U) Information in the call recordings comes from individuals that call CJIS business entities which could include any government source.					

(U) Non-government sources					
Members of the public	X	Public media, internet		Private sector	X
Commercial data brokers					
Other (specify): (U) Information in the call recordings comes from individuals that call CJIS business entities which could include any non-government source.					

2.3 (U) Analysis: Now that you have identified the information collected and the sources of the information, please identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Please describe the choices that the component made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

(U) Two types of information are retained in ETIS, a phone directory of personnel at the CJIS Division and call information and recordings of calls to and from those individuals. Both types of PII present risks to privacy concerning the accuracy of information maintained in the system. In order to mitigate this risk, ETIS limits searchable data fields to the minimum amount of information necessary to properly log the call and identify points of contact for further investigation.

(U) Information captured from the phone directory on personnel at the CJIS Division includes the name of the individual and the extension number the ETIS assigns to the individual. This information is collected based on information that may be vetted by the individual prior to its inclusion in the phone directory. Because ETIS generates call logs based on the assigned extension, there is a risk that the CJIS personnel identified in the call logs may not be the individual who was actually on the call. Identification of the individual can be verified through direct contact with the individual.

(U) Information concerning outside individuals falls into two subcategories, data that is automatically collected, such as the ANI, and the content of the audio recording. If the individual is calling from a number registered to him- or herself, the ANI could link back to the outside individual if further research is performed outside ETIS. Information concerning the owner of the ANI is not captured in ETIS, which limits the risk that ETIS records will misidentify an individual. Information provided throughout the course of the conversation about the outside individual is collected directly from the subject individual, which reduces the risk that information will be incorrect. There is a risk that information provided by the outside individual about others could be incorrect. However, none of the information provided throughout the course of the call is content searchable within ETIS and call recordings are kept for a limited amount of time unless deemed relevant to an investigation and transferred to an outside system.

(U) Section 3: Purpose and Use of the System

3.1 (U) Indicate why the information in the system is being collected, maintained, or disseminated. (Check all that apply.)

(U) Purpose			
X	For criminal law enforcement activities		For civil enforcement activities
	For intelligence activities	X	For administrative matters
	To conduct analysis concerning subjects of investigative or other interest		To promote information sharing initiatives
	To conduct analysis to identify previously unknown areas of note, concern, or pattern.		For administering human resources programs
	For litigation		
X	Other (specify): (U) The phone directory and call logs are maintained for administrative and record keeping purposes. Call recordings are maintained for quality assurance purposes and to meet business needs of the specific business entities. For example, incoming calls to the PAL may be used for law enforcement or intelligence investigation purposes.		

3.2 (U) Analysis: Provide an explanation of how the component specifically will use the information to accomplish the checked purpose(s). Describe why the information that is collected, maintained, or disseminated is necessary to accomplish the checked purpose(s) and to further the component's and/or the Department's mission.

(U) The ETIS maintains a call log of all incoming and outgoing phone calls from the CJIS division. This information is collected for record keeping purposes to track the CJIS division's telephonic communications. The information can be used, if necessary, to recreate the CJIS division's contacts with the public and with other governmental agencies. The internal phone directory supports the CJIS division by providing employees with a tool through which employees can contact each other for official purposes. Audio recordings of incoming calls to the business entities' call centers are collected for quality assurance purposes to ensure that the CJIS division is meeting customers' needs in a courteous and professional manner. Additionally, by recording incoming calls to the business entities' call centers, the CJIS division maintains a record of any threat made to a CSR via telephonic communication. This allows the CJIS division to provide the recorded threat to appropriate security personnel and investigatory authorities. Likewise, by maintaining audio recordings of incoming phone calls to the PAL unit on tips, major crime contacts, and weapons of mass destruction calls, the CJIS division is able, when necessary, to provide investigators with direct information for their investigations.

3.3 (U) Indicate the legal authorities, policies, or agreements that authorize collection of the information in the system. (Check all that apply and include citation/reference.)

	Authority	Citation/Reference
X	Statute	5 U.S.C. § 301; 44 U.S.C. § 3101; 28 U.S.C. § 533
	Executive Order	
	Federal Regulation	
	Memorandum of Understanding/agreement	
	Other (summarize and provide copy of relevant portion)	

3.4 (U) Indicate how long the information will be retained to accomplish the intended purpose, and how it will be disposed of at the end of the retention period. (Reference the applicable retention schedule approved by the National Archives and Records Administration, if available.)

(U) The ETIS call recordings are retained as required for the type of call center call. In accordance with legal requirements, call recordings for NICS are only retained for 24 hours and then purged. Call recordings for the PAL are maintained for 5 years. PAL calls remain within the ETIS for 13 months, after which time they can be restored to the ETIS from backup storage. Call recordings for the BSS CSG, the CJIS Help Desk, and Switchboard Operations are maintained for 30 days. General users' personal call logs retain the last 100 calls to or from the user's desk phone. General users can delete their personal call logs at any time. Call logs maintained within the ETIS are retained within the ETIS for 13 months and can be retrieved from backup storage for an additional year.

3.5 (U) Analysis: Describe any potential threats to privacy as a result of the component's use of the information, and controls that the component has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.) [In addition to providing a narrative answer, please consult the ISSO/ISSM for the system's NIST 800-122 PII Confidentiality Risk Level, and check the applicable Confidentiality Safeguard Security Controls.]

(U) Because the ETIS maintains PII in its call logs, call directory, and call recordings there is a risk that the PII could be improperly accessed, misused, or lost. To mitigate these risks, only minimal PII (personnel names and telephone extensions) is accessible to general users of the ETIS. More extensive PII data is stored within ETIS call recordings, but the content of these recordings is not searchable by personal identifier. The call recordings are only accessible from the FBI CJIS Unclassified Network (CJIS-UNET), specialized software within ETIS, and (for calls to PAL) through

the PALM database. CJIS-UNET workstations and access to the ETIS and PALM require two-factor authentication for access. Only specific CJIS-UNET users are granted access to the workstations that have access to the ETIS. Further, access to the call recordings is provided via web interfaces accessible via specialized software that requires another layer of authentication. Access to the call recording web interface is restricted to authorized personnel and ETIS system administrators. All FBI employees and contractors with access to ETIS are required to maintain an active, adjudicated security clearance. Also, all personnel are required to undergo annual privacy and information security training.

(U) PII Confidentiality Risk Level:

☐ **Low** ☐ **Moderate** ☑ **High**

- Is the system protected as classified; or
- Does the system involve intelligence activities, cryptologic activities related to national security, command and control of military forces, equipment that is an integral part of a weapon or weapons system; or
- Is the system critical to the direct fulfillment of military or intelligence missions (excluding routine business or administrative applications, e.g., finance, logistics, personnel management)?

☐ **Yes** ☑ **No**

If Yes, the system meets the NIST 800-59 definition of a National Security System.

(U) Access controls

X	Access Enforcement: General user access to the ETIS is restricted based on role-based access controls. Examples of these roles include customer service representatives, supervisors, and help desk users. Privileged access is restricted to authorized ETIS privileged users.
X	Separation of Duties: General users are separated by role that restricts the user's access.
X	Least Privilege: The ETIS general user roles are granted permissions that are the least required to perform the job role. Privileged access is restricted to authorized ETIS privileged users.
	Remote Access: Remote access to ETIS outside of FBI CJIS networks is prohibited except for the capability for an authorized user to access voice mail boxes from a public switched telephone.
	User-Based Collaboration and Information Sharing: The ETIS does not include any user collaboration or information sharing technologies.
	Access Control for Mobile Devices: The ETIS does not include mobile devices.
Access to the ETIS is limited from ETIS endpoint phones at CJIS Clarksburg and the NICS Call Centers and internal network access via CJIS-UNET. The ETIS recordings are only accessible from the FBI CJIS-UNET network, specialized software within the ETIS, or the PALM database. CJIS-UNET workstations and access to the ETIS and PALM require two-factor authentication for access. Access to CJIS-UNET and the ETIS are restricted to only authorized FBI users.	

(U) Audit controls

	Auditable Events: The ETIS call recorder software generates audit events for most instances when call recordings are replayed by authorized ETIS users. However, the ETIS QM software that is used to playback a very limited subset of recorded calls for quality purposes does not generate audit records when call recordings are replayed. Additionally, the ETIS call recorder software generates audit events for downloads of call recordings by a very limited set of authorized persons as a replay of the recording rather than distinguishing as a download event. Overall, ETIS does not generate audit records to fully satisfy FBI auditing requirements.
	Audit Review, Analysis, and Reporting:
Access to the ETIS is highly restricted thus reducing the risk of inappropriate or unauthorized user activity. The ETIS is only accessible via ETIS endpoint phones and via CJIS-UNET that are restricted to only authorized FBI users.	

(U) Identification and Authentication controls

X	Identification and Authentication: Access to ETIS user interfaces requires general users to authenticate using uniquely assigned identifiers. Access to ETIS user interfaces also requires logon to CJIS-UNET using a unique identifier and two-factor authentication. Not all privileged access to the ETIS uses unique attributable identifiers. Access to ETIS endpoint phone devices requires physical access to secured FBI CJIS facilities.
Privileged access to the ETIS is limited to ETIS privileged users. Shared privileged authenticators are controlled by ETIS system administrators and available to only a limited set of ETIS privileged users.	

(U) Media controls

	Media Access: The ETIS does not provide the capability to interface with removable media.
X	Media Marking: ETIS media is limited to media within the CJIS Data Center. The ETIS equipment in the CJIS Data Center is labeled with SF-710 Unclassified labels.
X	Media Storage: ETIS media is limited to media stored within the CJIS Data Center.
X	Media Transport: The ETIS does not include any removable media.
X	Media Sanitation: All ETIS media, upon removal, is sanitized and destroyed following FBI and CJIS Data Center sanitization policy and procedures. This includes degaussing and physical media destruction, as appropriate.

(U) Data Confidentiality controls

X	Transmission Confidentiality: Most ETIS communication paths are encrypted to protect confidentiality of sensitive information.
X	Protection of Information at Rest: Only the ETIS call recordings are encrypted at rest**.**
The ETIS communication paths that are not encrypted exist only within internal FBI networks that are protected by FBI boundary protections. ETIS data is stored only within FBI secure facilities thus greatly reducing the capability for unauthorized access to unencrypted ETIS data stored at rest.	

(U) Information System Monitoring

	Information System Monitoring: The ETIS inherits network services including network monitoring from the CJIS SEN.
Access to the ETIS is highly restricted thus reducing the risk of inappropriate or unauthorized user activity. The ETIS is only accessible via ETIS endpoint phones and via CJIS-UNET workstations that are restricted to only authorized FBI users.	

(U) Section 4: Information Sharing

4.1 (U) Indicate with whom the component intends to share the information in the system and how the information will be shared, such as on a case-by-case basis, bulk transfer, or direct access.

Recipient	How information will be shared			
	Case-by-case	Bulk transfer	Direct access	Other (specify)
Within the component	x		x	General users have direct access to their call logs and to the internal phone directories. Call recordings are accessed on a case-by-case basis by the business entity for which the call was recorded.
DOJ components	X			On a case-by-case basis, call recordings may be shared with law enforcement for investigative purposes.
Federal entities	X			On a case-by-case basis, call recordings may be shared with law enforcement for investigative purposes.
State, local, tribal gov't entities	X			On a case-by-case basis, call recordings may be shared with law enforcement for investigative purposes.
Public				
Private sector				
Foreign governments				
Foreign entities				
Other (specify):				

4.2 (U) Analysis: Disclosure or sharing of information necessarily increases risks to privacy. Describe controls that the component has put into place in order to prevent or mitigate threats to privacy in connection with the disclosure of information. (For example: measures taken to reduce the risk of unauthorized disclosure, data breach, or receipt by an unauthorized recipient; terms in applicable MOUs, contracts, or agreements that address safeguards to be implemented by the recipient to ensure appropriate use of the information – training, access controls, and security measures; etc.) [In answering the question, you should discuss the relevant NIST Confidentiality Safeguard Security Controls.]

(U) The ETIS does not include specific capabilities for information sharing. Access to ETIS endpoint phone devices requires physical access to secured FBI CJIS facilities. ETIS user interfaces are only accessible from CJIS-UNET by authorized ETIS users. CJIS-UNET requires two-factor authentication for access. Call recordings can be accessed only by authorized personnel from the business entities and ETIS system administrators. The majority of call recordings are not extracted from the ETIS where they are encrypted at rest. For those call recordings that are downloaded for business entity purposes, the recordings may be shared within the FBI. For investigative purposes, the PAL unit may share call recordings with FBI field offices or other agencies with the authority and jurisdiction to investigate the matters reported within the call recording. When specific call recordings are extracted from the ETIS, the business entities' established processes are used to control the handling of the extracted call recordings. Call recordings are only shared with and disclosed to those individuals or entities with a need to know in order to perform their authorized investigatory responsibilities.

(U) Section 5: Notice, Consent, and Redress

5.1 (U) Indicate whether individuals will be notified if their information is collected, maintained, or disseminated by the system. (Check all that apply.)

x	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 7.	
X	Yes, notice is provided by other means.	Specify how: For all recorded calls, the caller is notified at beginning of call that the call may be monitored or recorded.
	No, notice is not provided.	Specify why not:

5.2 (U) Indicate whether and how individuals have the opportunity to decline to provide information.

X	Yes, individuals have the opportunity to decline to provide information.	Specify how: All incoming calls to CJIS are voluntarily made. For the business entities for which calls are recorded, individuals are notified that the call may be monitored or recorded. Upon hearing the notification, the caller has the opportunity to hang up. Callers control what information they provide to CJIS during a call. The PAL accepts tips on an anonymous basis.
	No, individuals do not have the opportunity to decline to provide information.	Specify why not:

5.3 (U) Indicate whether and how individuals have the opportunity to consent to particular uses of the information.

	Yes, individuals have an opportunity to consent to particular uses of the information.	Specify how:
X	No, individuals do not have the opportunity to consent to particular uses of the information.	Specify why not: For calls that are recorded, all callers are informed via an automated message that the call may be monitored or recorded. By continuing the call after being notified of the recording, callers are implicitly providing consent for the recording; however, the specific uses of information depends on the type of call and the needs of the FBI.

5.4 (U) Analysis: Clear and conspicuous notice and the opportunity to consent to the collection and use of individuals' information provides transparency and allows individuals to understand how their information will be handled. Describe how notice for the system was crafted with these principles in mind, or if notice is not provided, explain why not. If individuals are not provided the opportunity to consent to collection or use of the information, explain why not.

(U) The ETIS collects minimal information in its call logs. For incoming calls, the ANI, if available, is collected which could possibly be traced back to a specific individual. For internal calls, only personnel's names and their extensions appear in the internal phone directory. All callers routed to a business entity for which calls are recorded hear an automated message informing them that the

call will be monitored or recorded. Callers who do not wish to have the call recorded have the opportunity to hang up. Moreover, callers control what information they provide during a call. The minimal information maintained in the call logs is kept for administrative and record keeping purposes. This privacy documentation and the System of Records Notices listed in Section 7 provide notice to the public on how the FBI may use information voluntarily provided to the FBI through telephone calls.

(U) Section 6: Information Security

(U) 6.1 Indicate all that apply.

X	A security risk assessment has been conducted.		
X	Appropriate security controls have been identified and implemented to protect against risks identified in security risk assessment. Specify: The ETIS requires two-factor authentication for privileged user access. All call recordings are encrypted at rest.		
	Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:		
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Certification and Accreditation: ETIS' current Authority to Operate expires on 5/18/2019.		
	(U) Auditing procedures are in place to ensure compliance with security standards. Specify, including any auditing of role-based access and measures to prevent misuse of information: Limited audits, as discussed in section 3 above, occur.		
X	Contractors that have access to the system are subject to provisions in their contract binding them under the Privacy Act.		
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOJ policy.		
X	The following training is required for authorized users to access or receive information in the system:		
	X	General information security training	
		Training specific to the system for authorized users within the Department.	
		Training specific to the system for authorized users outside of the component.	
	X	Other (specify):	All FBI personnel are required to take annual information security training.

6.2 (U) Describe how access and security controls were utilized to protect privacy and reduce the risk of unauthorized access and disclosure. [In answering the question, you should discuss the relevant NIST Confidentiality Safeguard Security Controls.]

(U) Only minimal PII is stored within the call logs and phone directory of the ETIS. Access to PII within the call logs and phone directory is restricted to personnel at the CJIS Division with direct access to phone devices or other restricted ETIS system interfaces. Access to ETIS endpoint phone devices requires physical access to secured FBI CJIS facilities. ETIS user interfaces are only accessible from CJIS-UNET by authorized ETIS users. CJIS-UNET requires two-factor authentication for access. Access to ETIS user interfaces requires an additional layer of authentication. Access controls for general users are defined using roles based on the user's job function that restrict access to only

necessary system functions. Most ETIS network communications are encrypted to protect sensitive data in transmission.

(U) The greatest risk to privacy comes from the potential misuse or loss of PII disclosed by callers and captured during the call recordings for CJIS business entities. As discussed above, the call recordings are only accessible from the FBI CJIS-UNET through specialized software within the ETIS or from the PALM database. CJIS-UNET workstations, the ETIS, and PALM require two-factor authentication for access. Only specific CJIS-UNET users are granted access to the workstations that have access to the ETIS. Further, access to the call recordings is provided via web interfaces accessible via the ETIS that require another layer of authentication. Access to the call recording web interface is restricted to authorized personnel and ETIS system administrators. ETIS call recordings are encrypted at rest. As discussed above, in the limited instances when a business entity needs to download a call recording for a business need, the call recordings are only shared with and disclosed to those individuals or entities with a need to know the information in the call recordings to perform their authorized investigatory or security responsibilities.

(U) Section 7: Privacy Act

7.1 (U) Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. (Check the applicable block below and add the supplementary information requested.)

X	Yes, and this system is covered by an existing system of records notice. Provide the system name and number, as well as the Federal Register citation(s) for the most recent complete notice and any subsequent notices reflecting amendment to the system: *Correspondence Management Systems for the Department of Justice*, **DOJ-003**, 66 FR 29992 (June 4, 2001) as amended at 66 FR 34743 (June 29, 2001), 67 FR 65598 (Oct. 25, 2002), and 82 FR 24147 (May 25, 2017); *Employee Directory Systems for the Department of Justice*, **DOJ-014**, 74 FR 57194 (Nov. 4, 2009) as amended at 82 FR 24151, 153 (May 25, 2017); *The FBI Central Records System*, **DOJ/FBI-002**, 63 FR 8659 (Feb. 20, 1998) as amended at 66 FR 8425 (Jan. 31, 2001), 66 FR 17200 (Mar. 29, 2001), and 82 FR 24147 (May 25, 2017); *The Next Generation Identification (NGI) System*, **DOJ/FBI-009**, 81 FR 27283 (May 5, 2016) as amended at 82 FR 24151, 156 (May 25, 2017); *National Instant Criminal Background Check System (NICS)*, **DOJ/FBI-018**, 63 FR 65223 (Nov. 25, 1998) as amended at 65 FR 78190 (Dec. 14, 2000), 66 FR 6676 (Jan. 22, 2001), 66 FR 8425 (Jan. 31, 2001), 66 FR 12959 (Mar. 1, 2001), and 82 FR 24147 (May 25, 2017).
	Yes, and a system of records notice is in development.
	No, a system of records is not being created.

7.2 (U) Analysis: Describe how information in the system about United States citizens and/or lawfully admitted permanent resident aliens is or will be retrieved.

(U) Information within the phone directory is retrieved by first or last name. Information in personal call logs is maintained in chronological order. Information in the master call log database can be retrieved by date of call, time of call, ANI, or CJIS employee name or phone extension. Call recordings are retrieved by CSR name or agent identification number, date and time of call, or ANI (if available). For calls into the PAL, call recordings can also be retrieved by UCID.